UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

MN

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/681,203	02/21/2001	Ariel Katz	158520.01	5124

22971 7590 03/19/2007
MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WA 98052-6399

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	03/19/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 03/19/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

roks@microsoft.com
ntovar@microsoft.com
a-rydore@microsoft.com

Office Action Summary	Application No.	Applicant(s)	
	09/681,203	KATZ ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 February 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-10,12-14,16-24 and 26-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-10,12-14,16-24 and 26-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01 February 2007 has been entered.

2. Claims 1, 4-10, 12-14, 16-24, and 26-36 have been presented for examination.

3. Claims 2, 3, 11, 15, and 25 have been cancelled as per Applicant's request.

Response to Amendment

##. The declaration filed on 01 February 2007 under 37 CFR 1.131 is sufficient to overcome the Perlman reference. Upon further consideration, a new ground of rejection is made in view of Jardin and Ranger.

##. See further rejections that follow.

Claim Rejections - 35 USC § 103

##. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

##. Claims 1, 4-10, 12-14, 16-24, and 26-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,681,327 to Jardin, hereinafter Jardin in view of U.S. Patent No. 6,393,568 to Ranger et al., hereinafter Ranger.

##. As per claims 1 and 33, Jardin teaches a method comprising:

receiving encrypted data at a proxy from a client over an unsecure network wherein the receiving completes a first hop and the proxy is an ending point of a first communication associated with the first hop (Figure 3 [block 310], column 6, lines 4-31);

decrypting the encrypted data into decrypted data (Figure 3 [block 330], column 6, line 58 to column 7, line 5);

re-encrypting the examined decrypted data (Figure 3 [block 336], column 7, lines 13-19); and

sending the re-encrypted data from the proxy to an origin server over a given network wherein the sending starts a second hop and the origin server is an ending point of a second communication associated with the second hop (Figure 3 [block 338], column 7, lines 13-19).

##. Jardin does not disclose examining the decrypted data for security purposes.

##. Ranger teaches examining the decrypted data for security purposes (column 2, lines 29-46).

##. It would have been obvious to one of ordinary skill in the art at the time the invention was made to examine the decrypted data for security reasons, since Ranger states at column 2, line 67 to column 3, line 15 that analyzing the decrypted data can prevent a virus from being unknowingly unleashed as the file is first encounter by the system, providing the advantage that performance penalties of the overall analysis are minimized for online systems.

##. Regarding claim 4, Jardin teaches wherein the given network is a secure network (column 7, lines 6-19, i.e. secure connection between the broker and server).

##. With regards to claims 5 and 16, Jardin discloses wherein the sending is in accordance with one of the hypertext transport protocol (HTTP), the post office protocol (POP), the wireless access protocol (WAP), or the Internet messaging access protocol (IMAP) (column 2, line 1, column 8, line 55).

##. Regarding claim 6, Jardin teaches wherein the given network is one of the unsecure network and a second unsecure network (Figure 3 [blocks 340-346], column 3, lines 48-51, column 5, lines 38-57).

##. Regarding claims 7 and 17, Jardin teaches wherein the receiving is within a secure socket layer (SSL) session (Figure 2, column 4, lines 34-58).

##. Regarding claims 8 and 19, Jardin teaches wherein the unsecure network is the Internet (Figure 1 [block 150], column 3, lines 49-50).

##. Regarding claims 9 and 24, Jardin teaches wherein the origin server is an effective origin server (Figure 1 [blocks 130a, 130b, 130c], column 3, line 61 to column 4, line 10).

##. Regarding claims 10 and 23, Jardin teaches wherein the client is an effective client (Figure 1 [block 110], column 4, lines 35-47).

##. Regarding claims 12 and 26, Ranger teaches wherein the method is performed by a firewall within the given network (column 4, lines 2-3, column 5, lines 41-43).

##. Regarding claims 13 and 27, Ranger teaches a computer-readable medium (claims 33-36) having a computer program stored thereon for execution by a processor (claims 25-32, claims 37-39).

##. As per claim 14, it is a well-known and common practice to receive unencrypted data from a client over a secure network and Official Notice of such is hereby taken.

##. Jardin teaches that after the data has been found not to pose a security risk,

encrypting the unencrypted data into encrypted data (Figure 3 [block 336], column 7, lines 13-19); and

sending the encrypted data (Figure 3 [block 338], column 7, lines 13-19) to an origin server over an unsecure network (Figure 3 [blocks 344, 346], column 7, lines 38-57).

##. Jardin does not teach examining unencrypted data for security purposes.

##. Ranger discloses examining the unencrypted data for security purposes (column 2, lines 29-46).

##. It would have been obvious to one of ordinary skill in the art at the time the invention was made to examine the decrypted data for security reasons, since Ranger states at column 2, line 67 to column 3, line 15 that analyzing the decrypted data can prevent a virus from being unknowingly unleashed as the file is first encounter by the system, providing the advantage that performance penalties of the overall analysis are minimized for online systems.

##. Regarding claim 18, Jardin teaches wherein the secure network is a carrier network (Figure 1 [block 150], column 3, lines 24-33).

##. Regarding claim 20, Jardin teaches wherein the client is a thin client (Figures 1 and 2 [block 110], column 3, lines 46-60).

##. Regarding claim 21, Jardin teaches wherein the client is one of a: personal digital assistant (PDA) device, a laptop computer, a notebook computer, and a wireless phone (Figures 1 and 2 [block 110], column 3, lines 46-60). The client disclosed by Jardin can be any one of a PDA, a laptop, notebook, or a wireless phone and official notice of such is hereby taken.

##. Regarding claim 22, Jardin teaches wherein the secure network is one of a wireless network or a wired network (column 3, lines 57-60). One of ordinary skill in the art would clearly recognize the physical layer of any network is either a wired or wireless network.

##. As per claims 28 and 31, Jardin teaches a system comprising:

a client to send encrypted data over an unsecure network and be a starting point of a first hop (Figure 3 [block 310], column 6, lines 4-31);

a proxy (i.e. broker) within a secure network to receive the encrypted data (Figure 3 [block 310], column 6, lines 4-31), decrypt the encrypted data into decrypted data Figure 3 [blocks 330, 340], column 6, line 58 to column 7, line 5, column 7, lines 38-57), and send the decrypted data over the secure network (Figure 3 [blocks 344, 346], column 7, lines 20-57), wherein the proxy is an ending point of a first communication associated with the first hop and a starting point of a second communication associated with a second hop (Figure 3 [blocks 342, 344], column 7, lines 20-57); and,

an origin server within the secure network to receive the decrypted data and be an ending point of the second communication associated with the second hop (Figure 3 [block 350], column 7, lines 44-57).

##. Jardin does not disclose perform a test relative to the decrypted data, and in response to a particular result transmitting the data.

##. Ranger teaches scanning the decrypted data for viruses and other potential malware (column 2, lines 29-46).

##. It would have been obvious to one of ordinary skill in the art at the time the invention was made to perform a test on the decrypted data and pending the result transmit the data to the server, since Ranger states at column 2, line 67 to column 3, line 15 that analyzing the decrypted data can prevent a virus from being unknowingly unleashed as the file is first encounter by the system, providing the advantage that performance penalties of the overall analysis are minimized for online systems.

##. Regarding claim 29, Jardin discloses a second client within a second secure network (Figure 1 [block 110], column 3, lines 47-50). It is a well-known and common practice to send and receive unencrypted data over a secure network and Official Notice of such is hereby taken.

##. Jardin discloses a proxy within the secure network to encrypt the unencrypted data into encrypted data (Figure 3 [block 336], column 7, lines 13-19), and send the encrypted data over an unsecure network in response to the test yielding a particular response (Figure 3 [block 338], column 7, lines 13-19).

##. Ranger teaches performing a test relative to the unencrypted data (column 2, lines 29-46).

##. Regarding claim 30, Jardin discloses a second client (Figure 1 [block 110], column 3, lines 47-50) to send second encrypted data over the unsecure network in an additional hop (Figure 3 [block 310], column 6, lines 4-31);

a proxy to receive the encrypted data (Figure 3 [block 310], column 6, lines 4-31), decrypt the encrypted data into decrypted data(Figure 3 [block 330], column 6, line 58 to column 7, line 5), encrypt the decrypted data into encrypted data (Figure 3 [block 336], column 7, lines 13-19), and send the encrypted data over the unsecure network (Figure 3 [block 338], column 7, lines 13-19).

##. Ranger teaches performing a test relative to the decrypted data (column 2, lines 29-46).

##. Regarding claim 32, Jardin discloses a second proxy within a second secure network to receive encrypted data (Figure 3 [block 310], column 6, lines 4-31), decrypt the encrypted data into decrypted data (Figure 3 [blocks 330, 340], column 6, line 58 to column 7, line 5), and send the decrypted data over the secure network (Figure 3 [blocks 344, 346], column 7, lines 38-57); and

a second origin server within the second secure network (Figure 1 [blocks 130a, 130b, 130c]) to receive the decrypted data (column 7, lines 38-57).

##. Regarding claim 34, Jardin teaches wherein the first network is a secure network (Figure 2, column 4, lines 34-47).

##. Regarding claim 35, Jardin teaches wherein the second network is an unsecure network, such that sending the data to the origin server over the second network in the second hop comprises first encrypting the data (Figure 3 [blocks 336, 338], column 7, lines 6-19).

##. Regarding claim 36, Jardin teaches wherein the second network is a secure network (Figure 3 [blocks 336, 338], column 7, lines 6-19).

Conclusion

##. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

##. The following patents are cited to further show the state of the art with respect to intermediary authentication, such as:

United States Patent No. 6,993,651 to Wray et al., which is cited to show securing a connection via SSL through an intermediary device.

United States Patent No. 6,952,768 to Wray et al., which is cited to show securing a connection via SSL through an intermediary device.

United States Patent No. 6,052,785 to Lin et al., which is cited to show client authorization to access remote data repositories through a middle tier server.

United States Patent No. 6,092,191 to Shimbo et al., which is cited to show packet authentication at a security gateway.

##. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

##. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

##. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100